APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/538,556	06/13/2005	Bonnie C. Sexton	US02 0576 US	5050

65913   7590   01/15/2010
NXP, B.V.
NXP INTELLECTUAL PROPERTY & LICENSING
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER
PYZOCHA, MICHAEL J

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
01/15/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 November 2009*.

2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2 and 4-19* is/are rejected.

7)☒ Claim(s) *3* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   Amendment filed 11/12/2009 has been received and considered.

2.   Claims 1-19 are pending.

Priority

3.   Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged. Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 U.S.C. 119(e) as follows:

The later-filed application must be an application for a patent for an invention which is also disclosed in the prior application (the parent or original nonprovisional application or provisional application). The disclosure of the invention in the parent application and in the later-filed application must be sufficient to comply with the requirements of the first paragraph of 35 U.S.C. 112. See *Transco Products, Inc. v. Performance Contracting, Inc.*, 38 F.3d 551, 32 USPQ2d 1077 (Fed. Cir. 1994).

The disclosure of the prior-filed application, Application No. 60433365, fails to provide adequate support or enablement in the manner provided by the first paragraph of 35 U.S.C. 112 for one or more claims of this application. The provisional application fails to provide an enabling disclosure for claims 1-18 of the present invention as it merely contains ideas the applicant's intend to perform without any explanation how the ideas will be fulfilled. Specifically, each independent claim contains affine and inverse affine transformations which are not even mentioned in Application No. 60433365 and

each dependent claim that further limits the invention are additionally not described in

60433365. Therefore, claims 1-18 are not given the priority claimed in Application No.

60433365 to December 13, 2002.

The priority claims to Application No. 60473527 to May 27, 2003 is proper and

the claims have been examined with respect to this date.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims 1, 2, 4, 5, 8-10, 12-15, 18 and 19 rejected under 35 U.S.C. 103(a) as

being unpatentable over Van Buer (US 20030198345) in view of Okada et al. (US

20030108195).

As per claims 1, 4, 5, 12 and 14, Van Buer discloses an apparatus for encryption

and decryption by performing a SubByte function of the Rijndael Block Cipher,

comprising: an S-box constructed by composing a first and second transformation,

wherein the first transformation is a look-up table for the multiplicative inverse in the

finite field GF(2^8), and performing a non-linear byte substitution using the composed S-

Box (see paragraphs [0067]-[0069]) and the second transformation is, a transformation

that performs one of an affine and inverse affine transformation based on a load pattern

(see paragraphs [0067]-[0069] and [0083]-[0088] where the load pattern is the data

used by the multiplexers to decide how the data is routed).

Van Buer fails to explicitly disclose the affine and inverse affine transformations

are combined into a single circuit.

However, Okada et al. teaches sharing the circuit for encryption as the circuit for

decryption (see paragraph [0186] where it is known that the affine and inverse affine

transforms are used for encryption and decryption respectively).

At the time of the invention it would have been obvious to a person of ordinary

skill in the art to combine the affine and inverse affine circuits in the Van Buer reference.

Motivation to do so would have been to further reduce the scale of the circuit

(see Okada et al. paragraph [0186]).

As per claims 2 and 18, the modified Van Buer and Okada et al. system

discloses the look-up table is the multiplicative inverse in the finite field $GF(2^8)$ (see Van

Buer paragraph [0068]), the affine-all transformation is implemented using a

combinational logic circuit (see Van Buer Fig. 4), that in the look-up table has {00}

mapped to itself (see Van Buer Table 1 on page 6).

As per claim 8, the modified Van Buer and Okada et al. system discloses a

plurality of instances of a data processing module arranged in a data processing

pipeline (see Van Buer paragraph [0067]).

As per claim 9, the modified Van Buer and Okada et al. system discloses the

apparatus is arranged to perform encryption or decryption in accordance with the

Rijndael Block Cipher, and wherein the data processing module is arranged to implement a Rijndael round (see Van Buer paragraphs [0064] and [0069]).

As per claim 10, the modified Van Buer and Okada et al. system discloses the data processing module is arranged to implement the SubByte transformation of the Rijndael round using the look-up table composed with the affine transformation for encryption and the inverse affine transformation for decryption (see Van Buer paragraphs [0067]-[0069]).

As per claims 13 and 15, the modified Van Buer and Okada et al. system discloses means for obtaining the multiplicative inverse is a look-up table and said means for performing the affine-all transformation is a combinational logic circuit (see Van Buer paragraphs [0067]-[0069] and [0083]-[0089]).

As per claim 19, the modified Van Buer and Okada et al. system discloses the use of a load pattern to decide which transform to apply to the input data (e.g. paragraph [0068] the data used by the multiplexer) fails to explicitly disclose that the load patterns are the same number of bits as the input data. However, one of ordinary skill in the art recognizes that there are a finite number of input sizes available to such a circuit can handle to obtain the predictable result of deciding which transform to use. Furthermore, the AES/Rijndael algorithm is performed on standard size blocks so it would be obvious to one of ordinary skill in the art to use the same size load pattern as the input block size because of the predictable results.

6.   Claims 6, 7, 11, 16 and 17 are rejected under 35 U.S.C. 103(a) as being
unpatentable over the modified Van Buer and Okada et al. system as applied to claims
1, 4, 5, 10 and 14 above, in view of Dent (US 5091942).

        As per claims 6, 7, 11, 16 and 17, the modified Van Buer and Okada et al.
system fails to explicitly disclose the look-up table is implemented in ROM.

        However, Dent teaches the use of ROM for a look-up table (see column 26 lines
29-48).

        At the time of the invention it would have been obvious to a person of ordinary
skill in the art to store the lookup table of the modified Van Buer and Okada et al.
system in ROM and for the circuit to implement the equations.

        Motivation, as recognized by one of ordinary skill in the art, to do so would have
been to allow the values of the table to be read but not changed.

Allowable Subject Matter

7.   Claim 3 is objected to as being dependent upon a rejected base claim, but would
be allowable if rewritten in independent form including all of the limitations of the base
claim and any intervening claims.

8.   The following is a statement of reasons for the indication of allowable subject
matter: The prior art fails to teach the implementation of the specific equations as put
for in claim 3 in combination with the remaining limitations.

Response to Arguments

9.   Applicant's arguments with respect to claims 1-19 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

10.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Stein, Morioka, and Yup teach methods of combining the encryption and decryption circuitry.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOCHA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 3:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Michael Pyzocha/
Primary Examiner, Art Unit 2437